



# The IPython Notebook

*Behind every great analysis is a  
great story*

Eric M. Hutchins  
*Lockheed Martin Fellow  
Chief Intelligence Analyst, LM-CIRT*

# About me

- **Lockheed Martin Computer Incident Response Team**
  - Net defense for the global LM enterprise
- **What has shaped me as an analyst the most...**
  - **The threats I've faced**
    - Battling advanced threats at LM since 2003
  - **The friends I've made**
    - DoD, law enforcement, intel community
    - Defense industry, Telecom, Energy, Finance

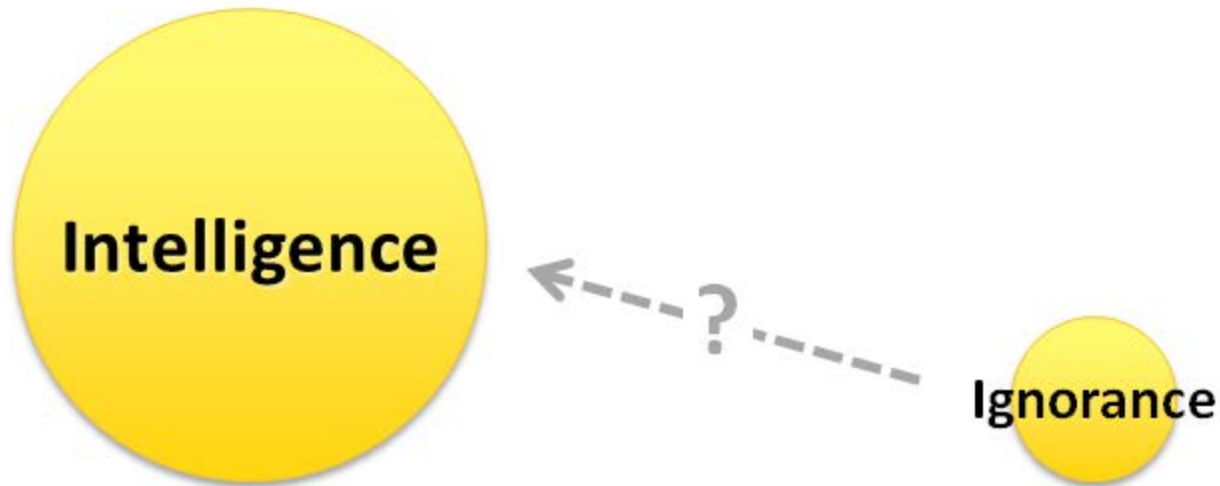
# **Intelligence-Driven Computer Network Defense** *Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*

Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.

6th Annual International Conference on Information Warfare  
and Security, Washington, DC, 2011.

<http://bit.ly/killchain>

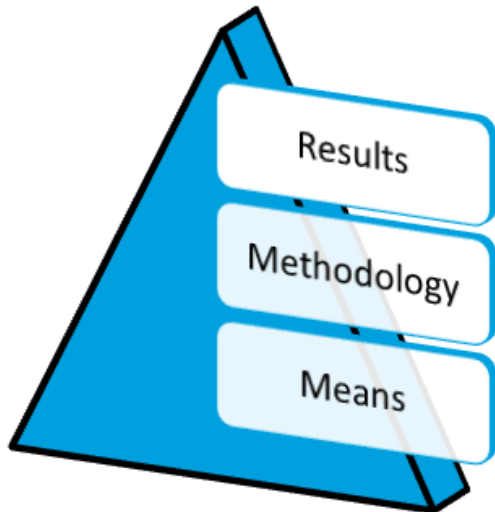
# Gaining Intelligence



*How do we make this a repeatable, scalable, team-wide process?*

# Common Challenges

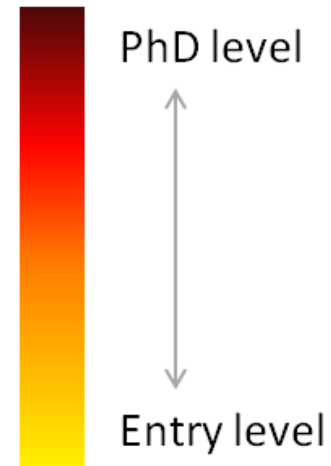
## *Depth of Documentation*



## *Instant Obsolescence*

graph.png  
graph\_latest.png  
graph\_latest2.png  
graph\_new.png  
graph\_updated.png

## *Varying Skill Levels*



# Components of Analysis



Raw data



Commentary



Sigs/IOCs



Code/Scripts



Tables



Visualizations

# IPython Notebook

## About

- *Interactive* computing platform
- Open source project
- IPy Notebook integrates code, text, headings, rich output in web display
- Language-agnostic
  - Back-end kernels for languages other than Python

## Learn more

- GitHub
  - <http://github.com/ipython/ipython>
- Example notebooks
  - <http://nbviewer.ipython.org>
- Install options
  - Continuum Analytics' Anaconda
    - <http://continuum.io>
  - Homebrew or pip

Fernando Pérez, Brian E. Granger, *IPython: A System for Interactive Scientific Computing*, Computing in Science and Engineering, vol. 9, no. 3, pp. 21-29, May/June 2007, doi:10.1109/MCSE.2007.53. URL: <http://ipython.org>

# The Vision

*Raw data, logs, forensic images, malware, etc*

**Search, Transform, Manipulate**

**IPython  
Notebook**



Commentary



Sigs/IOCs



Code/Scripts



Tables

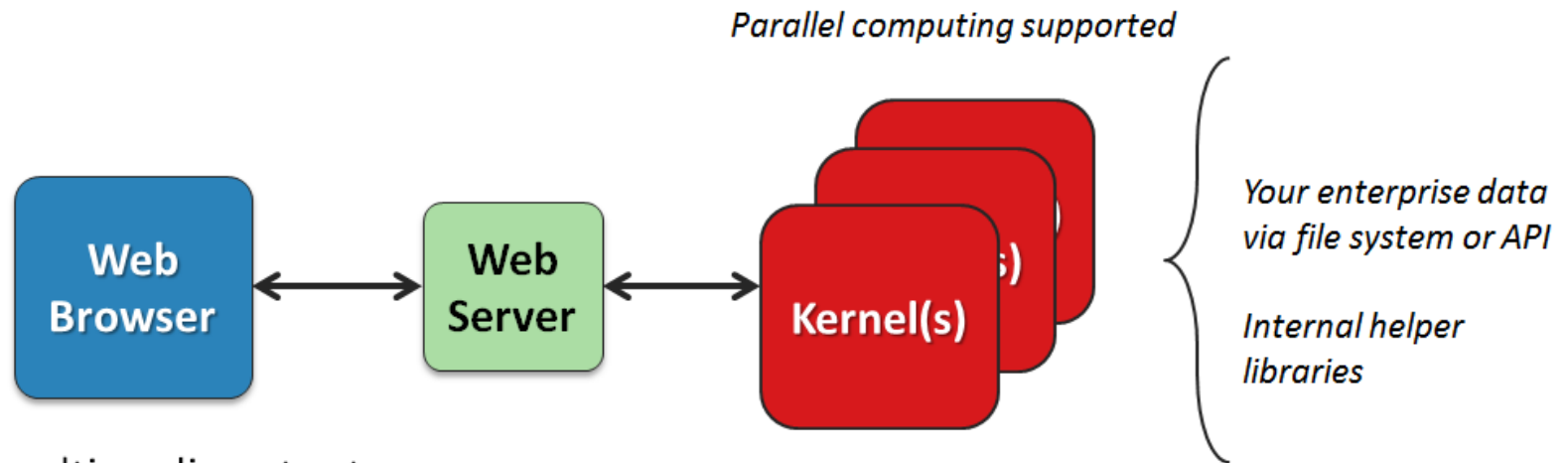


Visualizations

**Share, Extend, Improve, Teach**

*Yourself, your teammates, your community*

# IPython Architecture



Rich, multimedia output  
Notebooks are JSON files  
Currently only single-user supported

Coming soon: interactive  
Javascript widgets

Native kernel languages:  
Python, Julia, Ruby

Python hooks for:  
Bash, Perl, R, etc

Demo time